

REMARKS/ARGUMENTS

Claims 1-19 and 28-45 are pending in the present application. A telephone interview was conducted on July 13, 2004, between Examiner Thomas Ho, Applicant Joseph Fontana, and Applicant's Attorney, Stephen Sullivan. Applicant acknowledges and appreciates the helpful comments by the Examiner to facilitate allowance of the present application. In the interview, the difference between Caputo, the primary reference, and the independent claims were discussed, namely:

- The present invention authorizes a computer to use items of protected information, such as software and data, whereas Caputo's device authorizes a user to access a network (see the preambles of the independent claims).
- The device of the present invention is capable of storing multiple items of authorization information, such as keys, that are associated with respective items of protected information on the computer (e.g., claims 28, 32, and 1). Caputo's device stores encryption keys, but the keys are only used to encrypt/decrypt communications and are not associated with items of protected information. Caputo also teach the use of a PIN, but the pin is not stored in the device, or associated with items of protected information on a computer. Instead, the PIN is associated with the user.
- The device of the present invention performs the authorization, whereas in Caputo, the device merely encrypts the user's PIN and transmits it to a challenger on the network, and the challenger performs the authorization of the PIN.
- During the interview, the Examiner queried the online *Dictionary of Computing* for a definition of "Dongle," which is

/dong'gl/ n. 1. A security or copy protection device for proprietary software ..., which must be connected to an I/O port of the computer while the program is run. Programs that use a

dongle query the port at startup and at programmed intervals thereafter, and terminate if it does not respond with the dongle's programmed validation code. ... this innovation was necessary to allow daisy-chained dongles for multiple pieces of software.

However, Applicant points out that such a dongle fails to teach or suggest the present invention for several reasons. The primary reason is that to protect multiple pieces of software with a convention dongle, multiple dongles must be daisy-chained together, whereas in the present invention, only one device is necessary because the device of the present invention is capable of storing multiple items of authorization information corresponding to the respective pieces of software or data.

The remaining areas of discussion will be discussed more fully below.

Claim Rejections

The Examiner rejected claims 1-19, 28-29, 31-33, 35-44 under 35 U.S.C. §102 as being anticipated by U.S. Patent No. 5,778,071 issued to Caputo et al. The Examiner also rejected claims 30 and 34 under 35 U.S.C. §103 as being obvious. Applicant respectfully disagrees.

Just as in the telephone interview, Applicant will first provide an overview of the present invention followed by an overview of Caputo. The differences between the claims and Caputo are then explained.

The present invention provides an authorization system in which a portable security device is removably coupled to a computer system to selectively authorize the use of computer programs on the host computer. The portable security device stores multiple items of authorization information that are used by the computer system to use the protected software programs and data. The portable security device includes a communication interface for communicating with multiple information authorities, such as software vendors, for downloading the authorization information to the portable security device for subsequent authorization of the

vendor's software or data. The authorization information is then stored within a memory in the portable security device.

In one embodiment, the type of authorization information stored in the portable security device includes secret keys, or dynamic key selectors for generating secret keys. The dynamic key selectors may be stored in encrypted form in the portable security device. Each item of authorization information stored in the device corresponds to a particular protected software program and is used to authorize use of only that program.

When the user wishes to authorize use of a protected program on the host computer, the user connects the portable security device to the computer system, using a USB port, for instance. The host computer initiates a challenge-response transaction with the portable security device to determine whether the security device contains the proper authorization information for the protected software program. The challenge message transmitted to the security device includes a key ID identifying the protected software program. In response, the security device retrieves the dynamic key selector corresponding to the key ID, decrypts the dynamic key selector, and generates a secret key from the dynamic key selector. The portable security device then transmits a response message to a host computer that is a combination of the challenge message and the generated secret key. The secret key in the response then authorizes the host computer to access the protected software program.

In contrast to the present invention, Caputo is directed to a portable security device having a network communication interface that provides encryption and authentication capabilities to protect data and restrict access to authorized users (col. 1, lines 10-15). The device integrates security and interface functions to be used as an access control means to another computer or network (col. 3, lines 39-43). The portable device can be used as an identifying token, a communications network interface, a data encryptor, a user, and device and/or message

authenticator. It provides an electronic token which can be carried by the user to quickly identify him or her to a network, to a computer system, or to an application program. The device contains a modem for connecting the device to a data transfer path, such as a telephone network (column 5, lines 7-15). The device will not permit communications to proceed until the device and optionally, the user, have been identified by the authenticator.

In operation, the device is connected to a network and waits for a challenge from the network or other security device. When the challenge is received, the device may prompt a user to enter a PIN. The PIN is then encrypted and the encrypted result is returned to the challenger to be checked. If the verification is not successful, then the challenger ends the communication session. If it is successful, then an acknowledgment is returned to the device and communications are enabled by the challenger so the network or computer is accessible (Col. 17, lines 30-56).

The device of the present invention and the device of Caputo have different purposes. The device of the present invention is intended for copy-protection of digital information (including software) on a computer, whereas Caputo's device protects access to a network by a particular device or user. These different purposes have led to different methods of protection.

The method that Caputo uses for protecting access to information is identification of the device or the user. If servers on a network can verify the single identity of the device and/or the user, then access is granted. Caputo's device does not have the intelligence to determine what multiple pieces of information on the computer the user is allowed to access or not. Access is ultimately controlled by the servers on the computer network, which verify the user's PIN, as described above.

This is contrasted by the device of the present invention, which alone selectively controls access to protected pieces of information on the computer based on authorization information

associated with the protected items that are stored within the device. For example, authorization #1 must be present in the device in order to gain access to information item #1 on the computer; authorization #2 must be present in the device in order to gain access to information item #2; etc. The device can hold many of these authorizations to allow access of many items of information. The identity of the device or the identity its user in no way plays a role in determining access to pieces of information, as in Caputo. In addition, a server and/or a network are not needed for the device of the present invention to grant access to the computer to use the protected information, as in Caputo.

As Caputo discloses a device for protecting access to a network through device/user identification, Caputo fails to teach or suggest the claimed invention, which authorizes the use of “software” and data on a computer, as claimed.

Insofar as Caputo’s device is for protecting access to a network through device/user identification and requires different methods/functionality to achieve that purpose, Caputo’s device fails to solve the problem solved by the present invention, which is how to authorize the use of “software” and data on a computer in a manner that even an authorized user cannot make usable copies of the information being protected for an unauthorized user.

Although Caputo teaches the use of well-known PINS, and encryption and decryption keys that are kept secret, the PINS and keys are not “associated” with data or programs on the computer system.

Therefore, Caputo also fails to teach or suggest portable security device having the capability of “receiving multiple items of authorization information (such as key selectors) associated with the multiple items of protected information,” and then authorize the computer to use one of the items of protected information “based upon the corresponding item of authorization information” stored in the memory,” as recited in claims 28, 32, and 36. Likewise,

Caputo fails to teach or suggest the similar recitations claims 1, 2 and 12-14: a device that can receive “first” and “second items of information,” each respectively “associated” with first and second items of protected information, which are provided by a “vendor.”

Caputo also fails to teach or suggest a portable security device for "selectively authorizing the computer system to use multiple items of protected information" to be executed on the computer system, as recited in claim 28, or for selectively “authorizing” the host system to use the *one or more items of protected information* based upon the first or second items of authorization information being stored therein,” as recited in claim 1.

With respect to independent claim 14, the arguments above apply with full force and effect. In addition, claim 14 specifically recites “key selectors,” the function of which are neither taught or suggested by Caputo because Caputo’s PINs are not “associated with a first one of the items of protected information and provided by a vendor of the first one of the items of protected information,” as claimed.

With respect to claims 16-19, it is respectfully submitted that Caputo fails to teach or suggest a portable device that stores "one or more items of blended authorization information that are “derived from a plurality of items of authorization information.” As stated above, Caputo's PINS fail to provide the same function as the claimed items of authorization information. In addition, it is believed that Caputo's device does not store the user’s PIN therein, not to mention blending multiple ones of the PINS together.

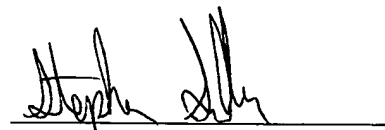
To the extent that the claims of the present invention recite “encryption,” it is noted that the Caputo device uses encryption/decryption on the information being protected. However, the purpose of Caputo’s encryption is to simply encrypt information as it travels over the network. In contrast, the device of the present invention does not encrypt/decrypt information that is protected and authorized. Instead, the protected information is stored on the computer awaiting

authorization. Because the method and purpose of the device of the present invention are different from those of the Caputo device, this functionally is not needed in the present invention.

In view of the foregoing, it is submitted that claims 1-19 and 28-45 are allowable over the cited references. Accordingly, Applicant respectfully requests reconsideration and passage to issue of claims 1-19 and 28-45 as now presented.

Applicants' attorney believes that this Application is in condition for allowance. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP



Stephen G Sullivan.
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540

July 14, 2004

Date